What is claimed is:

1. A method of encrypting an electronic file in an application program running in a suitable environment required for operating the program, comprising the steps of:

a) issuing a change document command to act upon the file;

b) intercepting the change document command;

c) acquiring an encryption key value;

d) encrypting the file using the encryption key value to create an encrypted file; and

e) completing the change document command by performing the change document command upon the encrypted file instead of the file.

2. A method as recited in claim 1, wherein step c) further comprises the steps of determining if the file should be encrypted, and if not, then skipping step d), and if so, then:

retrieving an encryption key name associated with the file; and

retrieving the encryption key value associated with the encryption key name.

3. A method as recited in claim 2, wherein there are plural encryption key values and at least one encryption key value associated with a user.

4. A method as recited in claim 3, comprising the further steps of:

requiring the user to submit to an access authentication step; and

if the access authentication step does not authenticate the user, then skipping steps c) and d), but if the access authentication step does authenticate the user, then retrieving the encryption key value associated with the encryption key name and the user.

5. A method as recited in claim 1, wherein steps steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of encryption algorithms;

selecting an encrpytion key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the algorithm and a data identifier associated with the file;

adding the file identifier to the file; and

using the key value and the algorithm to encrypt the file.

6. A method as recited in claim 5, comprising the further steps of:

selecting the file from within the contents of a second file that is larger than the file.

7. A method as recited in claim 6, comprising the further steps of:

creating a third file from the second file wherein the third file contains the encrypted file and the portion of the second file that does not include the file.

8. A method as recited in claim 7, wherein the encrypted file is located in a container.

9. A method as recited in claim 5, wherein the algorithm is selected from the plurality of encryption algorithms according to a preselected criteria.

10. A method as recited in claim 5, wherein the algorithm is selected from the plurality of encryption algorithms according to a preselected algorithm.

11. A method as recited in claim 5, wherein the file identifier is inserted into the file according to a preselected criteria.

12. A method as recited in claim 5, wherein the file identifier is inserted into the file according to a preselected algorithm.

13. A method as recited in claim 5, comprising the further step of:

invoking an option to initiate a virus scan program.

14. A method as recited in claim 5, comprising the further step of:

running a virus scan program on the file before it is encrypted.

15. A method of decrypting an electronic file that is to be opened in an application program running in a suitable environment required for operating the program, comprising the steps of:

a) issuing an open document command to act upon the file;

b) intercepting the open document command;

c) retrieving a decryption key value;

d) decrypting the file using the decryption key value to create an unencrypted file; and

e) completing the open document command by performing the open document command upon the unencrypted file instead of the file.

16. A method as recited in claim 15, wherein step c) further comprises the steps of determining if the file should be decrypted, and if not, then skipping step d), and if so, then:

retrieving a decryption key name associated with the file; and

retrieving the decryption key value associated with the decryption key name.

17. A method as recited in claim 16, wherein there are plural decryption key values and at least one decryption key value associated with a user.

18. A method as recited in claim 17, comprising the further steps of:

requiring the user to submit to an access authentication step; and

if the access authentication step does not authenticate the user, then skipping steps c) and d), but if the access authentication step does authenticate the user, then retrieving the decryption key value associated with the decryption key name and the user.

19. A method as recited in claim 15, wherein steps steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of encryption algorithms;

inputting a decrpytion key with a key value;

validating the decryption key value with the key value associated with a file identifier; and

using the key value and the algorithm to decrypt the file.

20. A method as recited in claim 19, comprising the further step of:

invoking an option to initiate a virus scan program.

21. A method as recited in claim19, comprising the further step of:

running a virus scan program on the decrypted file.

22. A method for encrypting and decrypting a file with one of a plurality of encryption algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of encryption algorithms;

selecting an encrpytion key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the algorithm and a data identifier associated with the file;

adding the file identifier to the file;

using the key value and the algorithm to encrypt the file and generate an encrypted file;

inputting a decryption key with a decryption key value;

validating the decryption key value with the key value associated with the file identifier;

using the key value and the algorithm to decrypt the file.

23. A method as recited in claim 22, comprising the further steps of:

uniquely identifying the encrpyted file with an encrypted data identifier during encrpytion; and

testing the encrypted data identifier after decrpytion by regenerating the encrypted data identifier and ascertaining that they are the same.

24. A method as recited in claim 22, comprising the further steps of:

selecting the file from within the contents of a second file that is larger than the file.

25. A method as recited in claim 24, wherein the encrypted file is placed in a container.

26. A method as recited in claim 26, comprising the further step of:

creating a third file from the second file wherein the third file contains the container and the portion of the second file that does not include the file.

27. A method as recited in claim 26, wherein the container is represented in the third file.

28. A method as recited in claim 27, wherein the decryption is initiated with whatever method is appropriate to the way the file is represented in the third file.

29. A method as recited in claim 27, wherein the second file is recreated from the third file after the file is decrypted.

30, A method as recited in claim 22, wherein the file is located in a document or image repository.

31. A method as recited in claim 22, comprising the further steps of:

sending the encrypted file from a first person to a second person over the Internet in an e-mail message.

32. A method as recited in claim 31, wherein the first person is the same as the second person.

33. A method as recited in claim 22, wherein the algorithm is selected from the plurality of encryption algorithms according to a preselected criteria.

34. A method as recited in claim 22, wherein the algorithm is selected from the plurality of encryption algorithms according to a preselected algorithm.

35. A method as recited in claim 22, wherein a portion of the file identifier is encrypted before it is inserted into the file.

36. A method as recited in claim 35, comprising the further step of decrypting a portion of the file identifier before the decryption key value is validated.

37. A method as recited in claim 36, wherein all of the file identifier is encrypted before the decryption key value is validated.

38. A method as recited in claim 22, wherein the file identifier is inserted into the file according to a preselected criteria.

39. A method as recited in claim 22, wherein the file identifier is inserted into the file according to a preselected algorithm.

40. A method as recited in claim 22, comprising the further step of:

invoking an option to initiate a virus scan program.

41. A method as recited in claim 22, comprising the further step of:

running a virus scan program on the file before it is encrypted.

42. A method as recited in claim 29, comprising the further step of:

running a virus scan program on the second file after it is recreated.

43. A method for encrypting a file with one of a plurality of encryption algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of encryption algorithms;

selecting an encrpytion key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the algorithm and a data identifier associated with the file;

adding the file identifier to the file; and

using the key value and the algorithm to encrypt the file and generate an encrypted file.

44. A method as recited in claim 43, comprising the further step of:

uniquely identifying the encrpyted file with an encrypted data identifier.

45. A method for decrypting an encrypted file with one of a plurality of encryption algorithms, comprising the steps of:

selecting an algorithm to use with the encrypted file from the plurality of encryption algorithms;

inputting a decryption key with a decryption key value;

validating the decryption key value with a key value associated with a file identifier that was added to a file during an encryption process that created the encrypted file; and

using the key value and the algorithm to decrypt the encrypted file.

46. A method as recited in claim 45, comprising the further step of:

testing an encrypted data identifier that is used to uniquely identify the encrypted file during the encryption process by regenerating the encrypted data identifier and ascertaining that they are the same.

Add a1

Add b